(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) Publication number : **0 599 558 A2**

(12) EUROPEAN PATENT APPLICATION

(21) Application number : **93309237.1**

(51) Int. Cl.[5] : **G07F 7/12**, G07C 9/00

(22) Date of filing : **19.11.93**

(30) Priority : **20.11.92 US 979018**

(43) Date of publication of application :
01.06.94 Bulletin 94/22

(84) Designated Contracting States :
DE FR GB NL

(71) Applicant : **PITNEY BOWES INC.**
World Headquarters
One Elmcroft
Stamford Connecticut 06926-0700 (US)

(72) Inventor : **Marcus, James R.**
1 Broad Court
Norwalk, Connecticut 06850 (US)

(74) Representative : **Cook, Anthony John et al**
D. YOUNG & CO.
21 New Fetter Lane
London EC4A 1DA (GB)

(54) Secure identification card and method and apparatus for producing and authenticating same.

(57) An identification card and method and apparatus for producing authenticating such an identification card. An object or other entity for which the identification card will evidence identity, status or characteristics is scanned to produce a digital signal which is compressed, encrypted, and coded as a two dimensional barcode or as some other appropriate form of coding, which is incorporated into one portion of the identification card. The image is also printed or otherwise embodied onto another portion of the identification card. A text message maybe appended to the signal before it is encrypted and also printed as plain text on the identification card. In one embodiment the signal representing the image is encrypted using a public key encryption system and the key is downloaded from a center. This key maybe changed from time to time to increase security. To facilitate authentication the corresponding decryption key is encrypted with another key and incorporated on the card. To validate the card the coded message is scanned, decoded, decrypted, expanded and displayed. The card may then be authenticated by comparison of the displayed representation of the image and the displayed text message with the image and text message printed on the card.

EP 0 599 558 A2

This invention relates to an identification card or similar item which serves as evidence of the identity or status of an object or other entity or person. More particularly, it relates to an identification card or similar item which has a high degree of security against forgery or tampering, and to methods and apparatus for producing and authenticating such cards.

(As used herein the term "identification card" will in general refer to an item similar to an identification badge of the type used by businesses to identify their employees, but it is within the contemplation of the invention, and as used herein the term "identification card" shall include, without limitation, documents, magnetic disks, CD's, or any other suitable item which may record an image together with related data and which may be associated with an object or other entity to be identified.)

The identification of objects or other entities is a problem as old as history. Isaac, blinded by age, mistakenly relied upon Esau's hairiness to distinguish him from Jacob, while Solomon was forced to threaten to kill a baby in order to identify its mother. History and fiction abounds with tales of letters, tokens, signets and passwords used to identify the bearer, and the consequences which have followed from their loss or forgery.

In modern times a common solution to this problem is the identification card which serves to establish the identity of the bearer, as well as usually some characteristic, status, or attribute of the bearer. Examples are the employee badge, as noted above, and, most commonly, a driver's licence. Typically, such identification cards will include a picture of the nominal bearer as well as relevant information in text and/or numeric form.

While identification cards and the like have generally proven useful for the day to day conduct of affairs nevertheless they are still subject to forgery or tampering, and indeed a moderately sized illegal industry exists for the purpose of providing false identification documents.

For applications where a high degree of security of identification is required, efficient techniques have been developed to recognize fingerprints, voice patterns, retinal patterns, or other characteristics of individuals. Such systems are highly successful in uniquely identifying individuals known to the system, but are subject to the disadvantages of requiring highly sophisticated, expensive sensors, which are typically not mobile, and which must be connected to a database which identifies selected individuals in terms of physical characteristics such as fingerprints. Such a database must generally be centrally located, both to protect it from tampering and to facilitate updating. Thus, these sophisticated systems are generally limited to restricting access to secure areas.

As is apparent from the above discussion the most common application of identification cards is to identify persons. However, the problem of identification may extend to a very broad class of objects or other entities. Thus, it may be desirable to be able to establish that a particular item has been inspected, or passed through customs, or was produced by a particular company. Similarly, it may be desirable to have secure evidence of the provenance of an art work, or the pedigree of an animal, or that a person, animal, or plant is free from disease. Such applications, and others which will be apparent to those skilled in the art are within the contemplation of the subject invention.

Perhaps because it relates to information, rather than tangible objects, the identification or authentication of documents or other forms of information has been dealt with perhaps more successfully in the past; usually by use of some form of encryption. Thus, U.S. patent no. 4,853,961; for: "Reliable Document Authentication System": to: Pastor; issued: August 1, 1989, discloses a system wherein a document is authenticated by encryption using a public key encryption system. U.S. patent no- 4,637,051; to Clark discloses a postage meter having an indicia which is authenticated by encryption. Many other applications of encryption to authenticate information will be known to those skilled in the art.

Thus, it is an aim of the subject invention to provide an identification card to identify an object or other entity, which card is secure against tampering and forgery.

In accordance with the invention there is provided a method and apparatus for producing an identification card and for validating that identification card. Apparatus for producing an identification card includes a scanner for producing a first signal representative of an image of the object or other entity to be identified, and a printer responsive to the scanner for printing the image on a first portion of the identification card. The apparatus further includes an encrypter for encrypting a second signal, which is derived, at least in part, from the first signal, and which includes a representation of the image; and a coder for incorporating a coded representation of the encryption of the second signal onto a second portion of the identification card.

Apparatus for validating an identification card so produced includes a reader for reading the coded representation of the second signal from the card, a decoder for decoding the coded representation of the second signal, a decrypter for decrypting the decoded signal, and a display for displaying the representation of the image incorporated in the second signal.

In accordance with the method of the subject invention the object to be identified is scanned to produce the first signal and a printer is controlled by the first signal to print the image of the object on the first portion of the identification card. The second signal, which is derived at least in part from the first signal,

and which includes a representation of the image is encrypted and coded and Incorporated in the second portion of the identification card.

Once produced the card is then validated by reading the coded representation of the second signal from the identification card, decoding and decrypting the second signal, and controlling a display in accordance with the decrypted second signal to display the representation of the image which is included in the second signal. The displayed representation of the image and the printed image on the first portion of the card are then compared to validate the card, and the printed image is compared to the object to confirm its identity.

In accordance with one aspect of the subject invention the first signal is converted into a digital signal for processing.

In accordance with another aspect of the subject invention the second signal includes a compressed form of the first signal.

(Signal compression is well known to those skilled in the art and, in the case of digital signals, involves the application of a predetermined algorithm to a signal to reduce the number of bytes which must transmitted or processed, while still retaining substantially all of the information represented by the signal.)

In accordance with another aspect of the subject invention the second signal is encrypted using an encryption key E_I, for a public key encryption system.

In accordance with still another aspect of the subject invention a decryption key, D_I which correspondences to the key, E_I, is encrypted with a second encryption key, E_1, for the public key encryption system, and the resulting encrypted decryption key $E_1[D_I]$, is appended to the encrypted second signal prior to incorporation of the second signal into the second portion of the identification card.

In accordance with still another aspect of the subject invention the encrypted second signal is printed on the second portion of the identification card as a two dimensional bar code.

In accordance with another aspect of the invention the apparatus for validating the identification card stores a decryption key D_1, corresponding to key E_1 and the decryption of the encrypted second signal includes the step of decrypting the encrypted key, $E_1[D_I]$, using the decryption key, D_1, to obtain the decryption key D_I, which may then be used to decrypt the encrypted second signal.

In accordance with a further aspect of the invention the second signal includes a text message and the text message includes a password which is known to a person who is to be identified by the identification card.

In accordance with yet a further aspect of the invention the second signal includes a text message which is also printed in plain text form on the first portion of the identification card.

Thus, it can be seen that the invention provides a method and apparatus for producing an identification card which includes an image which may be easily compared to the object or other entity whose identity is to be verified, and which is highly resistant to forgery or tampering. Other advantages of the invention will be readily apparent to those skilled in the art from consideration of the attached drawings and the detailed description set forth below.

The invention will be better understood from the following non-limiting description of an example thereof given with reference to the accompanying drawings in which:-

Figure 1 is a schematic block diagram of one example of an apparatus for producing an identification card in accordance with the invention;

Figure 2 is a schematic block diagram of an example of an apparatus for validating an identification card produced in accordance with the invention.

Figure 1 is a schematic block diagram of apparatus 10 for producing an identification card C. A person (or other object or entity) for whom the identification card is intended Is scanned by a conventional video scanner 12 to produce a first signal representative of that person's image. Preferably, the first signal is then converted to a digital form by an analog-to-digital convertor 14 for processing in the digital domain. It is however within the contemplation of the subject invention that at least the signal compression and encryption techniques to be described below may be carried out in the analog domain using signal compression and scrambling technologies well known to those in the analog signal processing arts.

The first signal is then input to a compression module 16 where it is compressed to reduce the amount of data which must be stored on identification card C.

It should be noted that where card C is to have substantially the same form as presently known identification cards, drivers licenses, etc. data compression is, at the present state of technology, necessary. However, with anticipated improvements in data storage technology, or in applications where the identification card may comprise a high capacity storage medium (e.g. a floppy disk), it is within the contemplation of the subject invention that the first signal may not require compression but that the full signal may be processed as will be described further below.

Data compression algorithms, specifically adapted for compression of video image signals, are known to those skilled in the art. Preferably, an algorithm known as the JPEG algorithm, which is known and commercially available is used in compressor 16. Further description of the operation of compressor 16 is not believed necessary to an understanding of the subject invention.

The compressed first signal is then input to an encrypter 20 to be included in the encrypted second signal which will be incorporated into identification card C, as will be described further below. Preferably encrypter 20 encrypts the second signal using an encryption key, E_I, for a public key encryption system such as the well known RSA system.

The encrypted second signal is then encoded in accordance with some predetermined format by coder module 22, which controls code generator 24 to incorporate the encoded encrypted second signal in a portion of identification card C.

In accordance with a preferred embodiment of the subject invention the coded signal is coded as a two dimensional barcode, such as the PDF-417 standard barcode, developed by the Symbol Technology Corporation of New York. However, the encrypted second signal may be coded into any suitable format. For example, for a smart card or a memory card coder 22 and code generator 24 may store the coded second signal as an appropriately formatted binary data block.

In the preferred embodiment where the coded second signal is represented as a two dimensional barcode the barcode will preferably be printed on back CB of identification card C.

In a preferred embodiment of the subject invention compressor module 16, encrypter module 20, and coder module 22 are implemented as software modules in a microprocessor; which is preferably, an Intel model 80386, or equivalent, or higher capacity microprocessor.

The digitized first signal is also input to printer 20 which may use any appropriate technology for the production of identification card C to print an image of the person O on front CF of identification card C. Front CF and back CB are then combined and laminated using well known technology by laminator 32 to produce identification card C.

In accordance with another preferred embodiment of the subject invention text input 30 is used to input a text message. In one embodiment of the subject invention at least a portion of the text message is combined with the compressed form of the first signal to form the second signal which is encrypted by encrypter module 20 and is also printed as plain text on the front CF of card C. Alternatively, text T may be compressed; as for example by deletion of control characters, which are restored in accordance with a predetermined format when text T is recovered, before text T is incorporated into the second signal. Thus, like image I text T is embodied in card C in both human recognizable form on the front CF and coded form on the back CB of card C. In another embodiment the text message may include a password P which would be encrypted and coded but which would not be printed in plain text on front CF.

In a preferred embodiment of the subject invention a center 40 transmits encryption code E_I to encrypter module 20. In order to increase the security of identification card C key E_I maybe changed from time to time. For the highest level of security key E_I maybe changed for each card C produced, or a different key may even be used to encrypt different portions of the second signal.

To facilitate decryption of the second signal in an environment where key E_I is frequently changed center 40 also transmits an encrypted decryption key $E_1[D_I]$ to be appended to the encrypted second signal by coder module 22. Thus, as will be seen below, when card C is to be validated the necessary decryption key D_I can be obtained by decrypting $E_1[D_I]$.

Typically, encryption/decryption pair E_1, D_1 will remain substantially constant during operation of system 10. However, in applications where system to is used to produced identification cards C for various organization different pairs E_1 D_1 may be used for different organizations.

Turning now to Figure 2 apparatus 50 for validating an identification card C is shown. The back CB of card C is scanned by a barcode scanner 52 having the capability to scan an appropriate two dimensional barcode. The scanned signal is then decoded by decoder module 54 and decrypted by decrypter module 58. In a preferred embodiment of the subject invention decrypter 58 stores decryption key D_1 which is used to decrypt encrypted key $E_1[D_I]$ to obtain decryption key D_I. Key D_I is then used to decrypt the decoded signal scan from card back CB.

Key D_1 is obtained by decrypter 58 from center 40. Typically, D_1 will remain constant during operation of system 50, as described above, and a direct communication link between system 50 and center 40 is not necessary and key D_1 maybe transmitted in any convenient manner. However, in one application, where identification card C has a predetermined expiration date it may be desirable to change key D_1 after the expiration date and if such expiration dates occur sufficiently often a direct communication link to center 40 maybe included in system 50.

The decrypted scan signal is then expanded in by an algorithm complimentary to the compression algorithm used in system 10, in a conventional manner which need not be described further for an understanding of the subject invention.

In a preferred embodiment of the subject invention decoder module 54, decrypter module 58, and expander module 60 maybe implemented as software modules in a microprocessor 61.

The decrypted, expanded signal is then displayed by a conventional display 62. The display includes a representation
RI of image I and the text message T which was included in the encrypted second signal scanned from card back CB. The display may also include a password P, which is known to the person O authorized to

have card C, but which is not included on card C, as described above. To validate the card image I is compared with its representation RI and the text message T as printed on card C and as shown on display 62 are compared. It should be noted that with compression representation RI will be somewhat degraded with respect to image I. It has been found however that using the above described JPEG algorithm a sufficiently accurate representation of an image of a person's face maybe coded as approximately 1,000 bytes of data and printed using the above described PDF-417 two dimensional barcode in an area of approximately 2.50 by 1.75 inches on the back of a substantially conventional wallet sized card. Of course, as described above, with improvements in storage technology and/or the use of media having a higher data storage capacity as embodiments of identification cards C representation RI can be arbitrarily close to image I.

In an embodiment incorporating a password, password P is shown on display 62 but, of course, is not printed on card front CF. Password P is known to person O authorized to have possession of Card C. Once card C is Validated by comparison of image I and text message T printed on card front CF with representation RI and the text message T as shown on display 62 then the identity of the person O carrying card C maybe confirmed by comparison of person O with image I, as well as testing person O for knowledge of password P. Text message T will then confirm the identity of person O and may also confirm the status or characteristics of person O.

The preferred embodiments described above have been given by way of example only, and other embodiments of the subject invention will be apparent to those skilled in the art from consideration of the detailed descriptions set forth above and the attached drawings.

Claims

1. A method of identifying an object, or other entity comprising the steps of:
   a) scanning said object or other entity to produce a first signal representative of an image of said object or other entity;
   b) printing said image on a first portion of an identification card;
   c) encrypting a second signal, comprising a representation of said image, said second signal being derived at least in part from said first signal;
   d) incorporating a coded representation of said encrypted second signal into a second portion of said identification card;
   e) reading said coded representation of said second signal from said identification card;
   f) decoding said second signal;
   g) decrypting said decoded second signal;
   h) inputting said decrypted second signal to a display to display said representation of said image;
   i) comparing said printed image to said displayed second image to validate said card; and
   j) comparing said printed image to said object or other entity to confirm its identity.

2. A method for producing an identification card, comprising the steps of:
   a) scanning an object or other entity to produce a first signal representative of an image of said object or other entity;
   b) printing said image on a first portion of said identification card;
   c) encrypting a second signal comprising a representation of said image, said second signal being derived at least in part from said first signal;
   d) incorporating a coded representation of said encrypted second signal into a second portion of said identification card.

3. A method according to claim 1 or 2 wherein said second signal comprises a compressed form of said first signal.

4. A method according to claim 1, 2 or 3 wherein said second signal is encrypted using an encryption key, E_I, for a public key encryption system.

5. A method according to any preceding claim wherein a decryption key, D_I, corresponding to said encryption key, E_I, is encrypted with a second encryption key, E_1, for said public key encryption system.

6. A method according to claim 5 wherein said encrypted decryption key, $E_1 [D_I]$, is appended to said encrypted second signal prior to incorporation into said second portion.

7. A method according to claim 3 or 6 wherein said representation of said encrypted second signal is incorporated into said second portion as a two dimensional bar code.

8. A method according to claim 7 wherein decryption of said encrypted second signal comprises the further steps of decrypting said encrypted key, $E_1 [D_I]$ using a decryption key, D_1.

9. A method according to claim 3 wherein said representation of said encrypted second signal is incorporated into said second portion as a two dimensional bar code.

10. Apparatus for producing an identification card, comprising:
    a) scanning means for producing a first signal representative of an image of an object or other entity to be identified by said identification card;
    b) printing means, responsive to said scanning means, for printing said image on a first portion of said identification card;
    c) encrypting means for encrypting a second signal, said second signal being derived at least in part from said first signal, and comprising a representation of said image; and
    d) coding means for incorporating a coded representation of said incryption of said second signal into a second portion of said identification card.

11. Apparatus according to claim 10 further comprising means for encrypting said second signal using an encryption key, E_I, for a public key encryption system.

12. Apparatus according to claim 11 wherein a decryption key, D_I, is encrypted with a second key, E_1, and said encrypted key E_1 $[D_I]$, is appended to said encrypted second signal prior to incorporation into said second portion.

13. Apparatus according to claims 10, 11 or 12 further comprising means for incorporating said representation of said encrypted second signal into said second portion as a two dimensional bar code.

14. Apparatus according to any of claims 10-13 further comprising means for receiving said encryption key, E_I, and said encrypted decryption key, E_1 $[D_I]$, from a central station.

15. A method for validating an identification card, said card having an image of an object or other entity to be identified on a first portion and a coded representation of an encrypted signal comprising a representation of said image incorporated on a second portion of said card, comprising the steps of:
    a) reading said coded representation or said signal from said card,
    b) decoding said coded representation of said signal;
    c) decrypting said encrypted representation of said signal; and,
    d) inputting said decrypted representation of said signal to a display for displaying said representation of said image; whereby,
    e) said card may be validated by comparison of said image on said first portion of said card with said displayed representation of said image.

16. A method according to claim 15 wherein said encrypted signal is encrypted using an encryption key, E_I, for a public key encryption system.

17. A method according to claim 16 wherein a decryption key, D_I corresponding to said key E_1, is encrypted with a second encryption key E_1 for said public key encryption system to form an encrypted decryption key, $E_1[D_I]$, and said encrypted decryption key, $E_1[D_I]$ is appended to said encrypted signal, and wherein said decryption step further comprises the steps of:
    a) decrypting said encrypted decryption key, $E_1[D_I]$ with a corresponding decryption key, D_1, to recover said decryption key D_I; and,
    b) decrypting said encrypted signal with said key, D_I.

18. Apparatus for validating an identification card, said card having an image of an object or other entity to be identified on first portion and a coded representation of an encrypted signal compressing a representation of said image incorporated in a second portion of said card, comprising:
    a) means for reading said coded representation of said signal from said card
    b) decoding means, responsive to said reading means for decoding said coded representation of said signal;
    c) decrypting means, responsive to said decoding means, for decrypting said decoded representation of said signal, and,
    d) display means, responsive to said decrypting means, for displaying said representation of said image; whereby,
    e) said card may be validated by comparison of said image on said first portion of said card with said displayed representation of said image.

19. An apparatus according to claim 18 wherein said encrypted signal is encrypted using an encryption key, E_I, for a public key encryption system.

20. Apparatus according to claim 19 wherein a decryption key, D_I, corresponding to said key E_I, is encrypted with an encryption key E_1 for said public key encryption system to form an encrypted decryption key $E_1[D_I]$, and said encrypted decryption key $E_1[D_I]$ is appended to said encrypted signal, and said decrypting means further comprises:
    a) means for decrypting said encrypted decryption key, $E_1[D_I]$ with a corresponding decryption key, D_1, to recover said decryption

key, D_i; and
b) means for decrypting said encrypted signal using said key, D_i.

21. An identification card, comprising:
a) a first portion having thereon an image of an object or other entity to be identified by said identification card; and,
b) a second portion incorporating an encoded representation of an encrypted signal comprising a representation of said image.

22. An identification card according to claim 21 wherein said digital signal is encrypted using an encryption key, E_i, for a public key encryption system.

23. An identification card according to claim 22 wherein a decryption key, D_i, corresponding to said encryption key, E_i, is encrypted with a second encryption key, E_1, for said public key encryption system to produce an encrypted description key, $E_1[D_i]$, and said encrypted decryption key, $E_1[D_i]$, is appended to said digital signal prior to incorporation into said second portion.

24. An identification card according to claim 23.wherein said representation of said encrypted digital signal is incorporated into said second portion as a two dimensional bar code.

25. An identification card according to claim 21 wherein said representation of said encrypted digital signal is incorporated into said second portion as a two dimensional bar code.

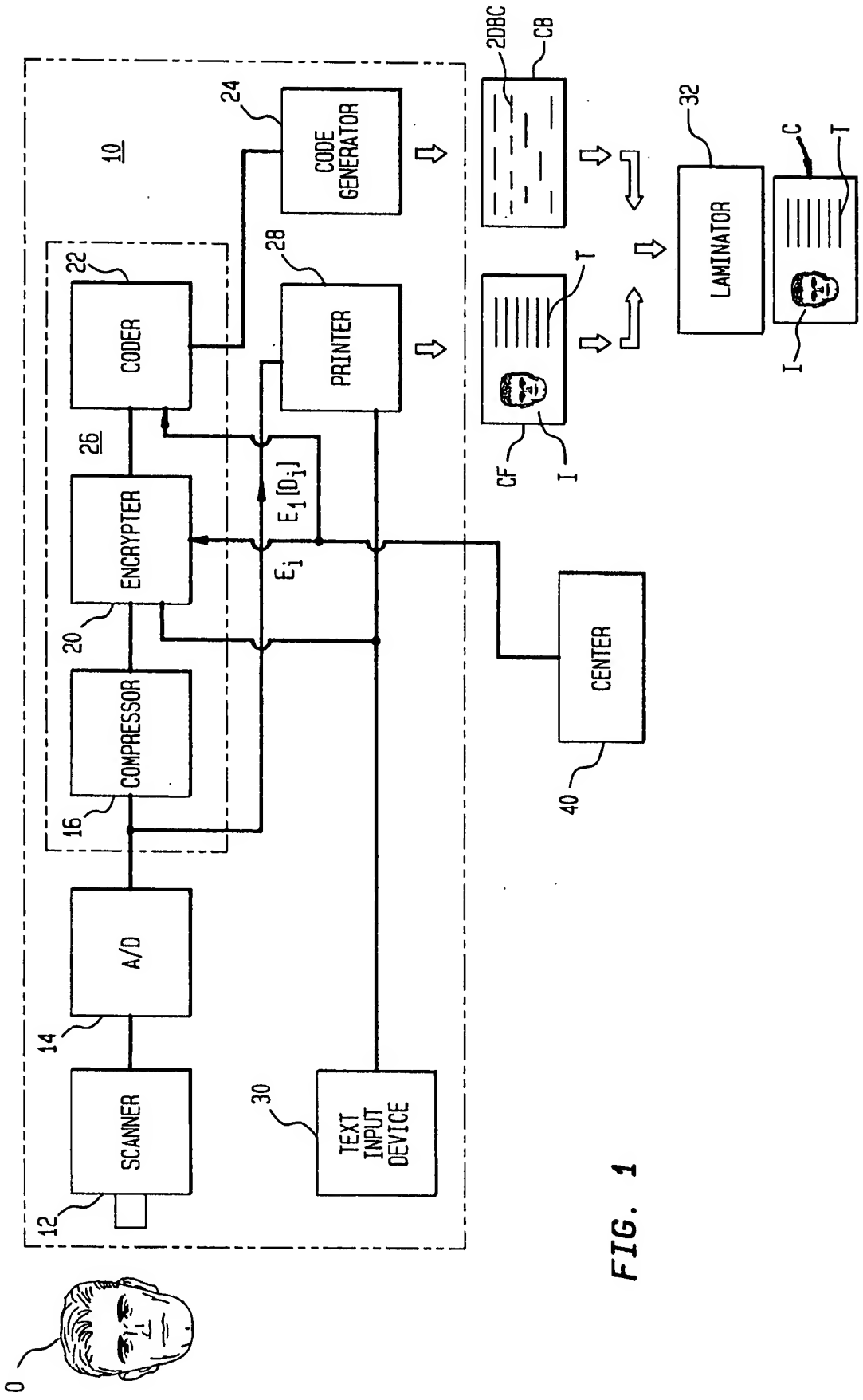
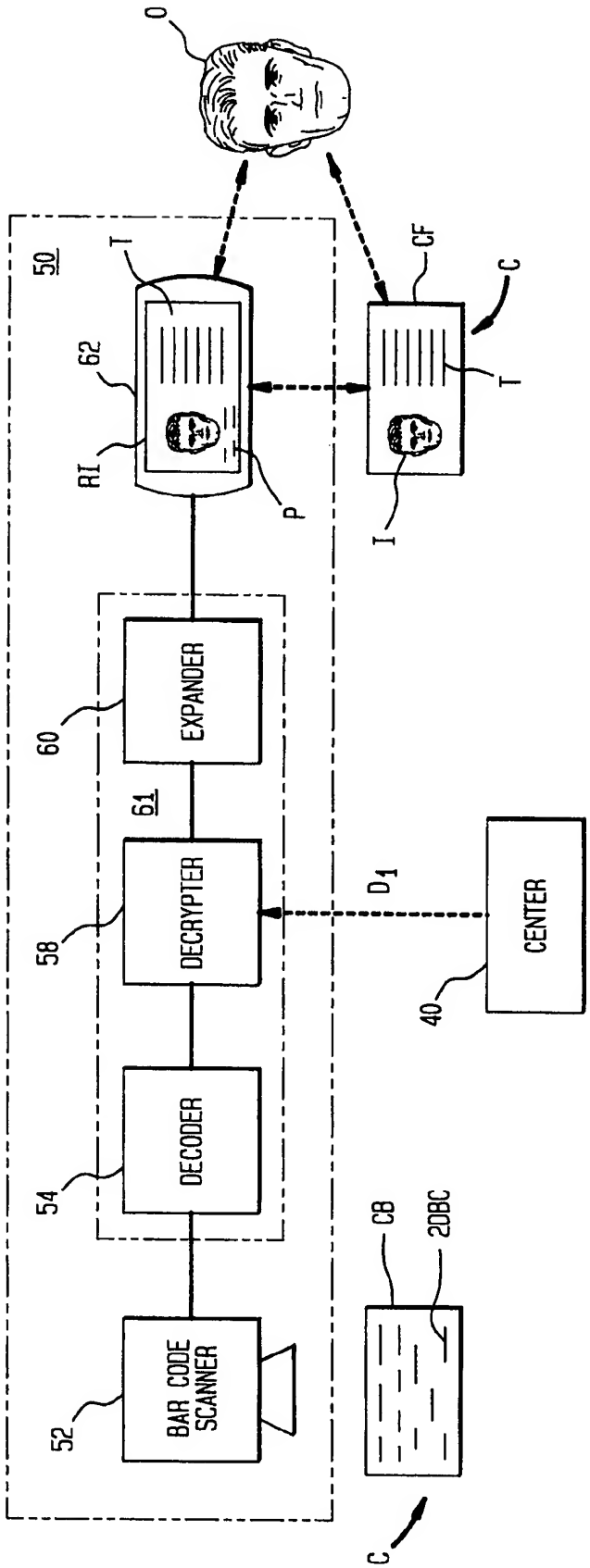

10
SCANNER
12
A/D
14
COMPRESSOR
16
ENCRYPTER
20
CODER
22
26
CODE GENERATOR
24
PRINTER
28
TEXT INPUT DEVICE
30
E_i
$E_1[D_1]$
CENTER
40
2DBC
CB
CF
I
T
LAMINATOR
32
C
I
T
0

FIG. 1

FIG. 2


O
50
T
62
RI
P
CF
C
T
I
EXPANDER
60
61
DECRYPTER
58
D_1
CENTER
40
DECODER
54
BAR CODE SCANNER
52
CB
20BC
C